Introduzione

L'Istituto di Informatica e Telematica ha da tempo un sistema di accreditamento e gestione degli utenti a cui si appoggiano i vari servizi dell'istituto. Attualmente è in corso una revisione e riprogettazione delle procedure di accreditamento e gestione degli utenti.
Il presente documento descrive le procedure attualmente in atto per la gestione degli utenti e la loro autorizzazione all'uso dei servizi informatici dell'istituto.

1. Descrizione del sistema

Il sistema di gestione degli utenti e delle identità digitali si compone di tre macchine utilizzate per ospitare un server database SQL, un server con LDAP master e una replica. Tutti gli inserimenti e modifiche sono fatte sul database SQL e sono riportate, da una procedura automatica, su LDAP. Inoltre è presente un server sul quale è implementato un Identity Provider usando il software Shibboleth. L'IDP è utilizzato per l'autenticazione Single Sign-On per l'accesso ai servizi messi a disposizione dalla Federazione IDEM.

2. Procedure e responsabilità dell'accreditamento utenti

L'accreditamento degli utenti viene gestito dall'Ufficio del Personale dello IIT. È infatti questo ufficio ad essere autoritativo relativamente alle informazioni sul personale afferente, nelle diverse forme, all'IIT. Un account viene rilasciato solo a chi ha un rapporto di lavoro contrattuale con l'istituto (tempo indeterminato, tempo determinato, collaboratori scientifici, assegnisti di ricerca, contratto interinale e contratto d'opera). Non sono rilasciati account a studenti che svolgono attivatà di tesi o stage e visitatori.

L'ufficio del personale inserisce i dati relativi all'identità e all'account tramite una interfaccia web nel database SQL. Per tutti i tipi di rapporto a tempo determinato viene inserita una data di scadenza.

Il meccanismo di autenticazione utilizzato si basa su username password. I nostri userid hanno il formato di nome.cognome. Inizialmente viene assegnata una password temporanea che l'utente può cambiare tramite una interfaccia web.

2.1 Utenti a tempo indeterminato

La procedura sopra descritta si applica a tutti gli utenti a tempo indeterminato per i quali non è prevista nessuna scadenza relativa all'account.

2.2 Utenti con rapporto di lavoro a scadenza

La procedura sopra descritta si applica anche a tutti gli utenti con rapporto di lavoro a tempo determinato. La validità dell'account ha una durata uguale a quella del contratto di lavoro che può essere rinnovabile senza limiti purché subordinatamente al rinnovo del contratto o di altro rapporto formale con l'Istituto.

2.3 Studenti e visitatori

Per gli studenti (tirocinanti, tesisti, dottorandi, specializzandi) e visitatori non sono rilasciati account.

3. Proroga scadenza account

Il rinnovo degli account con scadenza avviene semplicemente con una richiesta all'Ufficio del Personale. Sarà cura di quest'ultimo verificare che il richiedente ne abbia diritto in funzione della validità del proprio rapporto con IIT.

4. Disabilitazione account

La disabilitazione di un account può avvenire o direttamente per iniziativa dell'Ufficio del Personale, nel momento in cui il rapporto con IIT viene a cessare, o su richiesta dello stesso utente o di altro utente che ne abbia diritto (es. responsabile del contratto dell'utente, responsabile di un servizio, ecc.).

La disabilitazione dell'account, avviene anche automaticamente alla scadenza del contratto.

L'operazione non rimuove effettivamente i dati relativi all'account ma lo segnala come disabilitato in modo da conservare lo storico nel database SQL. Mentre la procedura automatica che esporta i dati in LDAP cancella i dati relativi agli account disabilitati.

5. Password

La password temporanea assegnata inizialmente (par. 2) dovrà essere cambiata dall'utente.
La password non ha scadenza. Il sistema registra la data dell'ultimo aggiornamento della stessa ed è quindi compito dell'applicazione che richiede l'autenticazione e necessita che sia prevista la scadenza delle password, verificare che l'intervallo di tempo dall'ultima modifica sia non superiore al periodo previsto per legge (D. L. 196/'03, tre mesi per dati personali, sei mesi per dati sensibili) e impedire l'accesso notificando il motivo all'utente. L'utente può modificare la propria password tramite interfaccia web.

6. Tipologia di utenza

La posizione contrattuale nei confronti dell'IIT è registrata nel database SQL e riportata automaticamente nell'attributo LDAP "EmployeeType" dell'Object Class "inetOrgPerson".
L'affiliazione, definita con l'attributo "primaryAffiliation" dell'Object Class "inetOrgPerson" richiesta da IDEM, non è salvata all'interno del database LDAP ma viene comunicata alla controparte (tramite un "mapping" dinamico eseguito da Shibboleth rispettando le corrispondenze dei valori definiti nel documento "Specifiche tecniche per la compilazione e l'uso degli attributi" della Federazione IDEM.

7. Il sistema di autenticazione e autorizzazione interno

I servizi interni dell'istituto utilizzano le credenziali descritte in questo documento per l'autenticazione e autorizzazione. Al momento non abbiamo servizi interni che usano meccanismi di web SSO.

8. Partecipazione ad altre federazioni

L'istituto partecipa alla federazione eduroam per l'accesso alle reti wifi di enti di ricerca e accademici.